

In response to the request that writing intensive courses should have directions on how to write, I am posting these “Proof writing notes”. This first note is about:

Proof by contradiction

We did an example of this in class and we will be doing many proofs by contradiction throughout the semester.

Step 1. As in any good proof, the plan of the proof should be given briefly at the beginning. You need to start by stating that you will prove the theorem by contradiction. Some people use the short sentence: “Assume by contradiction that the theorem is false” or simply “Suppose not.”

Step 2. At this point you need to state the *negation* of the conclusion statement. Note that this is one more assumption added to the list assumptions already given by the theorem.

Step 3. You write the body of the proof.

Step 4. You arrive at a contradiction. There are two basic types of contradictions:

a) You get a statement contradicting one of the assumptions of the theorem. If this happens you need to specify which assumption is being contradicted. For example you might write “Therefore, S has 3 elements which contradicts the assumption that it has an even number of elements.”

b) You get a statement contradicting a known fact. For example you might write “Therefore $2 = 3$ which is a contradiction.”

c) Another possibility is that you prove the theorem. This is also a contradiction because you assumed the theorem is false. If this happens you probably didn’t need to do the proof by contradiction.

Example

Theorem There are an infinite number of prime numbers.

Proof Suppose not. Then there are only finitely many prime numbers and we can list them in increasing order as p_1, p_2, \dots, p_n . Let m be the product of these prime numbers plus 1:

$$m = p_1 p_2 \cdots p_n + 1$$

Since 2 is prime, $m \geq 3$. Let k be the smallest integer which is greater than 1 and divides m . Then we claim that k is a prime number which is not in the list. This claim contradicts the assumption that we have a complete list of all primes. So, it suffices to prove the claim.

We prove the claim by contradiction. Suppose the claim is false. Then either k is not prime or it is equal to one of the primes p_i . The second case is not possible since any divisor of k will also divide m and p_i does not divide m since it divides $m - 1$. So, suppose that k is not prime. Then k is a product of two smaller numbers $k = ab$ which are both at least 2. Since k divides m so do a and b . This contradicts the minimality of k . This contradiction proves the claim and the theorem follows. QED.

Note: The “minimality of k ” refers to the assumption that k is the smallest integer which is ≥ 2 and divides m . The proof shows that a, b are ≥ 2 and divide m but are smaller than k which is a contradiction.